

IC CARD ISSUING SYSTEM, IC CARD PROCESSING SYSTEM, AND IC CARD

Veröffentlichungsnr. (Sek.) JP2000172490
Veröffentlichungsdatum : 2000-06-23
Erfinder : YAMADA HIROYOSHI
Anmelder : TOSHIBA CORP
Veröffentlichungsnummer : JP2000172490
Aktenzeichen:
(EPIDOS-INPADOC-normiert) JP19980341843 19981201
Prioritätsaktenzeichen:
(EPIDOS-INPADOC-normiert)
Klassifikationssymbol (IPC) : G06F9/06; G06K17/00
Klassifikationssymbol (EC) :
Korrespondierende Patentschriften

Bibliographische Daten

PROBLEM TO BE SOLVED: To expand and determine a specific area of a nonvolatile memory by allowing the IC card to divide an application recording area of its nonvolatile memory by physical addresses according to an indication from an issuing device.

SOLUTION: While a terminal device 11 specifies an issuer, the issue, card ID, slot size, etc., of the card are indicated and an IC card 12 which is not recorded is inserted into the card insertion slot 120 of a reader writer 112. The slot size is set according to an application made by a person who installs an application. Consequently, the card ID set by the terminal device 11 is recorded in a system data area 31 of the nonvolatile memory(EEPROM) 23 and the addresses and sizes in user application areas 35 by slots are recorded in a slot management table 34a in the card data area 34 of the EEPROM 23, so that a symbol indicating the state of the corresponding application is recorded.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-172490
(P2000-172490A)

(43) 公開日 平成12年6月23日 (2000.6.23)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)	
G 0 6 F 9/06	4 1 0	G 0 6 F 9/06	4 1 0 B	5 B 0 5 8
	5 5 0		5 5 0 Z	5 B 0 7 6
G 0 6 K 17/00		G 0 6 K 17/00	B	

審査請求 未請求 請求項の数 8 O L (全 10 頁)

(21) 出願番号 特願平10-341843

(22) 出願日 平成10年12月1日 (1998.12.1)

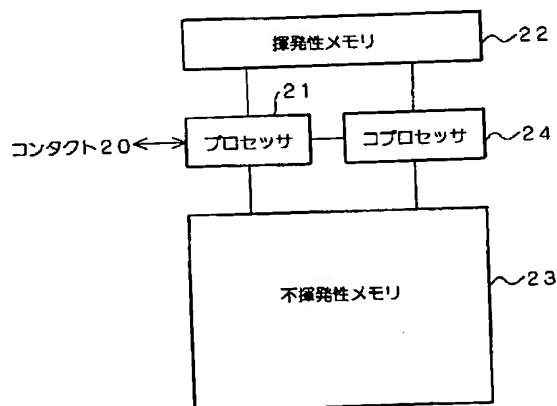
(71) 出願人 000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72) 発明者 山田 広佳
神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内
(74) 代理人 100058479
弁理士 鈴江 武彦 (外6名)
Fターム(参考) 5B058 CA13 CA25 KA11
5B076 AA02 AA17 AB02 AB10 FC07

(54) 【発明の名称】 ICカード発行システムとICカード処理システムとICカード

(57) 【要約】

【課題】 この発明は、アプリケーションが使用する領域をそのまま制限された物理領域にマッピングすることにより、領域管理をセキュリティ管理と連動させ、アプリケーションの独立性を領域監視により確保することができる。

【解決手段】 この発明は、発行後にアプリケーションのインストールが可能なICカードと、ICカードへの入出力手段となる端末装置を具備するICカードシステムにおいて、各アプリケーションが事前に確定されたスロット内でのみ領域を拡張しうるようにスロット領域を確定するようにしたものである。



【特許請求の範囲】

【請求項 1】 不揮発性メモリを有する IC カードと、この IC カードを発行する発行装置とからなり、この IC カードの発行後に、この IC カードの不揮発性メモリにアプリケーションのインストールが行える IC カード発行システムにおいて、

上記発行装置が、アプリケーションをインストールする領域確保の指示を行う指示手段を有し、上記 IC カードが、上記発行装置からのアプリケーション単位の領域確保の指示に基づいて、上記不揮発性メモリのアプリケーション記録領域を物理アドレスにより分割する分割手段を有することを特徴とする IC カード発行システム。

【請求項 2】 不揮発性メモリを有する IC カードと、この IC カードにアプリケーションをインストールする処理装置とからなる IC カード処理システムにおいて、上記処理装置が、上記 IC カードの所定のスロットへのアプリケーションのインストールを指示する指示手段と、この指示手段により指示されたアプリケーションを出力する出力手段とからなり、

上記 IC カードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記アプリケーションの記録を不許可とする手段とからなることを特徴とする IC カード処理システム。

【請求項 3】 アプリケーションがインストールされている不揮発性メモリを有する IC カードと、この IC カードにインストールされているアプリケーションを処理する処理装置とからなる IC カード処理システムにおいて、

上記処理装置が、上記 IC カードの所定のスロットのアプリケーションによる処理を指示する指示手段とからなり、上記 IC カードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、この実行手段により所定のアプリケーションの処理を実

行する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、

この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする手段とからなることを特徴とする IC カード処理システム。

【請求項 4】 複数のモジュールからなるアプリケーションがインストールされている不揮発性メモリを有する IC カードと、この IC カードにインストールされているアプリケーションを処理する処理装置とからなる IC カード処理システムにおいて、

上記処理装置が、上記 IC カードの所定のスロットのアプリケーションによる処理を指示する指示手段とからなり、

上記 IC カードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する第 1 の記憶手段と、上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、

この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記第 1 の記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する第 1 の判断手段と、

上記アプリケーション記録領域に記録されているアプリケーションのモジュールの利用を許可するアプリケーションを記憶する第 2 の記憶手段と、

上記第 1 の判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションのモジュールを利用すると判断した際に、上記第 2 の記憶手段に記憶されている許可条件に基づいて、そのモジュールの利用を許可するか否かを判断する第 2 の判断手段と、

この第 2 の判断手段により上記モジュールの利用を許可すると判断した際に、そのモジュールの処理を上記実行手段により実行し、上記第 2 の判断手段により上記モジュールの利用を許可しないと判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする手段とからなることを特徴とする IC カード処理システム。

【請求項 5】 アプリケーションがインストールされている不揮発性メモリを有する IC カードと、この IC カードにインストールされているアプリケーションの処理を指示する処理装置とからなる IC カード処理システムにおいて、

上記 IC カードが、

上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、
上記処理装置から指示された所定のアプリケーション記録領域に記録されているアプリケーションの処理を実行する際、または所定のアプリケーションをスロット内にインストールする際に、他のスロットへアクセスするアプリケーションであるか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、

この判断手段によりアプリケーションのインストールまたは実行を不許可とする手段とからなることを特徴とするICカード処理システム。

【請求項6】 アプリケーションをインストールする処理装置によってアプリケーションがインストールされる不揮発性メモリを有するICカードにおいて、

上記ICカードは、

上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、

上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、他のアプリケーションのスロットを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、

この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記アプリケーションの記録を不許可とする手段とからなることを特徴とするICカード。

【請求項7】 アプリケーションがインストールされている不揮発性メモリを有し、処理装置からの指示によりインストールされているアプリケーションを実行するICカードにおいて、

上記ICカードは、

上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、

上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、

この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、

この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする手段とからなることを特徴とするICカード。

【請求項8】 アプリケーションをインストールする処理装置によってアプリケーションがインストールされる

不揮発性メモリを有するICカードにおいて、

上記ICカードは、

上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、

上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、スロットを超過してアプリケーションが書込まれることを不許可とする手段を有することを特徴とするICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ICカードの発行後に、このICカードに対するアプリケーションのインストールが行えるICカード発行システムとICカード処理システムとICカードに関する。

【0002】

【従来の技術】従来のICカードは、マスクROMにアプリケーションを予め書込み、書き換え可能な不揮発性メモリEEPROMをデータ領域として使用している。

【0003】このようなICカードでは、アプリケーションを変更したり追加しようとした際に、新たにマスクROMを作り直したカードを発行（製造）しなければならず、開発期間や費用が掛かってしまうという問題がある。

【0004】そこで、ICカードの発行後に、このICカードに対するアプリケーションのインストールが行え、追加、削除、更新が行えるICカード処理システムが提案されている。このICカードでは、複数のアプリケーションが扱えるようになっている。

【0005】このシステムで用いられるICカードでは、各アプリケーションごとにアプリケーションのIDが定義されているものの、物理的なアドレスは管理されていないかった。

【0006】たとえば、図9に示すように、アプリケーションは、一般に複数の依存関係のあるソフトウェアモジュール（プログラムにおけるサブルーチンに対応）により構成される。図9の例では、3つのアプリケーション1、2、3が存在し、例えば、アプリケーション2はソフトウェアモジュール321、322、323、324により構成される。まず、アプリケーション2の入口として、ソフトウェアモジュール321を呼び出すことにより、要求に対する処理が開始される。ソフトウェアモジュール321は、その処理の中でソフトウェアモジュール322と323に部分的な処理を依頼する。ソフトウェアモジュール322は自身の処理を行い、その完了を依頼元であるソフトウェアモジュール321に通知する。また、ソフトウェアモジュール323は、さらにその部分的な処理をソフトウェアモジュール324に依頼し、その結果と自身の処理とを合わせて、依頼元であるソフトウェアモジュール321に通知する。ソフトウ

ェアモジュール321は全ての結果を回収し、自身の処理とを合わせて、アプリケーション2の全体としての結果を要求元に通知することになる。

【0007】他のアプリケーション、ソフトウェアモジュールも同様に作用する。

【0008】ここにおいて、アプリケーション1、2、3はソフトウェアモジュールの総体、として位置づけられる。また、上述の流れのなかで問題になるのは、ソフトウェアモジュール322と314の間に点線で示したようなアプリケーションを跨っての依存関係が定義される場合である。各アプリケーションは、異なる思想により、異なる設計者、異なる利益追求のために設計されていることが考えられ、不用意な他アプリケーションからの参照を許すと秘密漏洩、情報破壊などのセキュリティ弱化を引き起こしかねないと言う問題がある。

【0009】したがって、ICカードの発行後に、このICカードに対するアプリケーションのインストールが行えるICカード処理システムにおいて、上記ICカードが不揮発性メモリを有し、上記ICカードにおける各アプリケーションが、事前に確定された上記不揮発性メモリの所定領域内でのみ領域を拡張しうるようにスロット領域を確定することができるものが要望されている。

【0010】

【発明が解決しようとする課題】この発明は、ICカードの発行後に、このICカードに対するアプリケーションのインストールが行えるものにおいて、上記ICカードが不揮発性メモリを有し、上記ICカードにおける各アプリケーションが、事前に確定された上記不揮発性メモリの所定領域としてのスロット内でのみ領域を拡張しうるようにスロット領域を確定することができるICカード発行システムとICカード処理システムとICカードを提供することを目的としている。

【0011】

【課題を解決するための手段】この発明のICカード発行システムは、不揮発性メモリを有するICカードと、このICカードを発行する発行装置とからなり、このICカードの発行後に、このICカードの不揮発性メモリにアプリケーションのインストールが行えるものにおいて、上記発行装置が、アプリケーションをインストールする領域確保の指示を行う指示手段を有し、上記ICカードが、上記発行装置からのアプリケーション単位の領域確保の指示に基づいて、上記不揮発性メモリのアプリケーション記録領域を物理アドレスにより分割する分割手段を有するものである。

【0012】この発明のICカード処理システムは、不揮発性メモリを有するICカードと、このICカードにアプリケーションをインストールする処理装置とからなるものにおいて、上記処理装置が、上記ICカードの所定のスロットへのアプリケーションのインストールを指示する指示手段と、この指示手段により指示されたアプ

リケーションを出力する出力手段とからなり、上記ICカードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記アプリケーションの記録を不許可とする手段とからなる。

【0013】この発明のICカード処理システムは、アプリケーションがインストールされている不揮発性メモリを有するICカードと、このICカードにインストールされているアプリケーションを処理する処理装置とからなるものにおいて、上記処理装置が、上記ICカードの所定のスロットのアプリケーションによる処理を指示する指示手段と、この指示手段からなり、上記ICカードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする手段とからなる。

【0014】この発明のICカード処理システムは、複数のモジュールからなるアプリケーションがインストールされている不揮発性メモリを有するICカードと、このICカードにインストールされているアプリケーションを処理する処理装置とからなるものにおいて、上記処理装置が、上記ICカードの所定のスロットのアプリケーションによる処理を指示する指示手段と、この指示手段からなり、上記ICカードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する第1の記憶手段と、上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段と、この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記第1の記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する第1の判断手段と、上記アプリケーション記録領域に記録されているアプリケーションのモジュールの利用を許可す

るアプリケーションを記憶する第2の記憶手段と、上記第1の判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションのモジュールを利用すると判断した際に、上記第2の記憶手段に記憶されている許可条件に基づいて、そのモジュールの利用を許可するか否かを判断する第2の判断手段と、この第2の判断手段により上記モジュールの利用を許可すると判断した際に、そのモジュールの処理を上記実行手段により実行し、上記第2の判断手段により上記モジュールの利用を許可しないと判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする処理手段とからなる。

【0015】この発明のICカード処理システムは、アプリケーションがインストールされている不揮発性メモリを有するICカードと、このICカードにインストールされているアプリケーションの処理を指示する処理装置とからなるものにおいて、上記ICカードが、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置から指示された所定のアプリケーション記録領域に記録されているアプリケーションの処理を実行する際、または所定のアプリケーションをスロット内にインストールする際に、他のスロットへアクセスするアプリケーションであるか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段によりアプリケーションのインストールまたは実行を不許可とする手段とからなる。

【0016】この発明のICカードは、アプリケーションをインストールする処理装置によってアプリケーションがインストールされる不揮発性メモリを有するものにおいて、上記ICカードは、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、他のアプリケーションのスロットを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記アプリケーションの記録を不許可とする手段とからなる。

【0017】この発明のICカードは、アプリケーションがインストールされている不揮発性メモリを有し、処理装置からの指示によりインストールされているアプリケーションを実行するものにおいて、上記ICカードは、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からの指示を受入れ、この指示された所定のスロットに対応してアプリケーション記録領域に記録されているアプリケーションの処理を実行する実行手段

と、この実行手段により所定のアプリケーションの処理を実行する際に、他のアプリケーションを利用するか否かを上記記憶手段に記憶されているスロット単位の物理アドレスに基づいて判断する判断手段と、この判断手段により現在処理中のアプリケーションが記録されるスロットと異なるスロットに記録されているアプリケーションを利用すると判断した際に、上記実行手段による所定のアプリケーションの処理を不許可とする手段とからなる。

【0018】この発明のICカードは、アプリケーションをインストールする処理装置によってアプリケーションがインストールされる不揮発性メモリを有するものにおいて、上記ICカードは、上記不揮発性メモリのアプリケーション記録領域のスロット単位の物理アドレスを記憶する記憶手段と、上記処理装置からのアプリケーションを受入れ、アプリケーション記録領域の所定のスロットに記録する際に、スロットを超過してアプリケーションが書込まれることを不許可とする手段を有する。

【0019】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態について説明する。

【0020】図1は、この発明のICカード発行システムの概略構成を示している。

【0021】このICカード発行システムは、端末装置11とICカード12とにより構成される。端末装置11は、演算および人間からの入力を司る演算装置111と、ICカード12との入出力を司るリーダライタ112が結線113により接続されている。

【0022】演算装置111は、演算を行うためのプロセッサを持ち、また人間系を含む外部からの入力手段を持っている。ICカード12への要求と、結果ステータスの処理をここで行う。

【0023】リーダライタ112は、演算装置111より要求を受け、その要求をカード挿入口120に挿入されているICカード12へと発行する。同様にICカード12からのステータスを受け取り、その結果を演算装置111へと報告する。

【0024】また、ICカード処理システムも、上記ICカード発行システムと同じ構成となっている。

【0025】ICカード12は、図1、図2に示すように、外部との接点となるコンタクト20、および演算、制御を行うプロセッサ21、一時データを配置するための揮発性メモリ(RAM)22、永続的にデータを保存するための不揮発性メモリ(EEPROM)23を持つ。またコンタクト20を通じてリーダライタ112と通信を行う。上記不揮発性メモリ23としては、フラッシュメモリ、FRAM等を用いても良い。

【0026】プロセッサ21は、端末装置11からロードされるアプリケーションをICカード12用のカードアプレットCAPに変換する機能を有している。

【0027】上記プロセッサ21の制御のもと、2種類のメモリ、揮発性メモリ22と不揮発性メモリ23が管理される。また、特に負荷の生じる演算を行うためのコプロセッサ24を持つこともあり、これはプロセッサ21の指示のもと演算を行う。

【0028】データは、図1におけるコンタクト20より入力され、一般に揮発性メモリ22内に格納される。ここで受信されたデータは、プロセッサ21により解析され、処理される。ここで、保存が必要なデータはプロセッサ21の指示のもと不揮発性メモリ23に書き込まれ、特殊な演算が可能なものはコプロセッサ24へと処理の指示が送られる。また、RAM22では格納しきれない大きなデータなどが一時的に、EEPROM23の別領域に書き込まれることがある。

【0029】上記EEPROM23は、図3、図4に示すように、カードID等が記録されるシステムデータ領域31、領域チェック用のBCC領域32、コミットバッファ領域としてのCB領域33、スロットを管理するスロット管理テーブル34aやアプリケーション間の許可状態を示す共有テーブル34bが記録されるカードデータ領域34等のシステム領域と、複数スロットからなり各スロットごとにアプリケーションが記録できるユーザアプリケーション領域35とにより構成されている。BCC領域32は、カードデータ領域34、ユーザアプリケーション領域35の正しさをチェックするための領域である。

【0030】ユーザアプリケーション領域35は、たとえば、図4に示すように、#0～#7の8つのスロットにより構成されており、各スロット単位で、ユーザアプリケーションが記録されるようになっている。

【0031】上記カードデータ領域34に記録されるスロット管理テーブル34aは、図5に示すように、各スロットごとに、スロットに記録されるアプリケーションの状態STS、スロットに記録されるアプリケーション名(番号)AID、スロットのユーザアプリケーション領域35における先頭位置(アドレス)TOP、スロットのユーザアプリケーション領域35におけるサイズSIZEにより構成されている。

【0032】各スロットごとの先頭位置(アドレス)TOP、サイズSIZEは、カード発行者をカード発行機(ICカード発行システム)にて認定した際に、設定できるものである。

【0033】アプリケーションの状態STSとしては、アプリケーションの申請に基づくスロットの領域の設定時にICカード発行システムで「C」が記録され、ICカード処理システムでのアプリケーションのインストール時の準備段階時に「P」(Prepared)が記録され、ICカード処理システムでのICカードへのアプリケーションのインストール終了時に「R」(Registered)が記録されるようになっている。

【0034】上記カードデータ領域34に記録される共有テーブル34bは、図6に示すように、各アプリケーションのモジュールに対する参照を許可するアプリケーションが記録されるようになっており、許可を行うアプリケーション名AIDのモジュール名と許可されるアプリケーション名AIDによって構成されている。

【0035】上記ICカード発行システムにおいて、ICカード12を発行する際の処理について説明する。

【0036】すなわち、端末装置11において発行者を特定している状態において、カードの発行やカードIDやスロットサイズ等が指示されているとともに、未記録状態のICカード12がリーダライタ112のカード挿入口120に挿入されている。上記スロットサイズは、アプリケーションのインストーラ者からの申請に基づいて設定されるようになっている。

【0037】これにより、端末装置11により設定されたカードIDがEEPROM23のシステム領域31に記録され、端末装置11により設定されたスロットサイズに基づいてEEPROM23のカードデータ領域34のスロット管理テーブル34aに各スロットごとのユーザアプリケーション領域35における先頭位置(アドレス)TOPとユーザアプリケーション領域35におけるサイズSIZEとが記録され、対応するアプリケーションの状態STSに申請を示す「C」が記録される。

【0038】上述したスロットの管理は発行者により行われるようになっている。

【0039】上記ICカード処理システムにおいて、ICカード12にアプリケーションをインストールする際の処理について説明する。

【0040】すなわち、端末装置11においてアプリケーションのインストーラ者を特定している状態において、アプリケーションのインストールやアプリケーション名AIDや各アプリケーションのモジュールに対する許可アプリケーション等が指示されているとともに、上記ICカード発行システムで発行されたICカード12がリーダライタ112のカード挿入口120に挿入されている。

【0041】これにより、端末装置11により設定されたアプリケーション名AIDがEEPROM23のカードデータ領域34のスロット管理テーブル34aに現在申請されている状態のスロットに対応して記録され、対応するアプリケーションの状態STSに準備を示す「P」が記録される。

【0042】この状態において、端末装置11からICカード12アプリケーションがロードされることにより、ICカード12内のEEPROM23のユーザアプリケーション領域35にインストールされ、記録される。

【0043】この際、スロット管理テーブル34aの準備中状態のスロットに対応して記録されているユーザア

アプリケーション領域35における先頭位置(アドレス)TOPに基づいて、アプリケーションが記録される。また、アプリケーションのサイズは、スロット管理テーブル34aの準備中状態のスロットに対応して記録されているアプリケーション領域35におけるサイズSIZEに基づいて規定されている。

【0044】したがって、アプリケーション領域35におけるサイズSIZEを超過してスロット外にアプリケーションを書込もうとしたことが検出された場合は書き込みは不許可とされる。

【0045】上記アプリケーションがインストールされた後、スロット管理テーブル34aの対応するスロットのアプリケーションの状態STSに記録を示す「R」が記録される。

【0046】たとえば、上述したアプリケーションの設定により、図7に示すように、スロット#0に対してアプリケーション1が記録され、スロット#1に対してアプリケーション2が記録され、スロット#2に対してアプリケーション3が記録され、アプリケーション1がモジュール511~514からなり、アプリケーション2がモジュール521~524からなり、アプリケーション3がモジュール531~533からなる。

【0047】この状態において、所定のアプリケーションのモジュールに対する許可アプリケーションの指示に基づいて、カードデータ領域34の共有テーブル34bに、所定アプリケーションのモジュールに対する参照を許可するアプリケーションが記録される。

【0048】たとえば、図6に示すように、共有テーブル34bにアプリケーション1のモジュール514に対してアプリケーション2が記録され、図7に示すように、アプリケーション1のモジュール514に対してアプリケーション2(モジュール522)による利用が許可されるようになっている。

【0049】次に、各アプリケーション実行時のモジュールごとの領域確認処理(領域管理)について、図8に示すフローチャートを参照しつつ説明する。

【0050】すなわち、プロセッサ21は、所定のモジュールにおいて、他のモジュールの呼出しが行われた際に(ST1)、スロット管理テーブル34aを参照して現在のモジュールが属する領域(スロット)をその物理アドレスから確認するとともに、呼び出す他のモジュールが属する領域(スロット)をその物理アドレスから確認する(ST2)。この確認の結果、プロセッサ21は、それらが同一領域(スロット)か否かを判断し(ST3)、この判断の結果が同一領域の場合、プロセッサ21は、処理を継続する(ST4)。

【0051】上記ステップ3の判断の結果、同一領域(スロット)できない場合、プロセッサ21は、共有テーブル34bを参照して呼び出す他のモジュールに対する参照を許可するアプリケーションを確認することによ

り(ST5)、現在のモジュールが呼び出す他のモジュールを参照できるか否かを判断(権限判断)する(ST6)。この判断の結果、呼び出す他のモジュールにおいて参照を許可している場合、プロセッサ21は、処理を継続する(ST4)。

【0052】上記ステップ6の判断の結果、呼び出す他のモジュールが参照を許可していない場合、プロセッサ21は、処理の継続を否認し(アプリケーションの記録の不許可)、処理を終了する(ST7)。

【0053】これにより、アプリケーションの跨りを領域跨りとして検出できる。また現在のモジュールと呼び出す他のモジュールのそれぞれが配置されている物理情報により判別が行えるので、データ偽造、データ破壊等を考慮しても、より高いセキュリティが確保できる。また、従来システムのように対応表などを利用することなく、直接物理情報から決定できるのでより高速に処理が可能である。

【0054】上記領域確認処理を、所定のアプリケーションを用いて処理を実行している際に行っているが、アプリケーションのインストール時に行ってインストールを不許可として良い。

【0055】上記したように、スロットは明示的に領域管理と関係づけられ、インストールされるアプリケーションが使用できる最大領域として定義づけられる。このシステムでは、アプリケーションを入れるための器として定義されることになる。このため、各アプリケーション間の境界が明らかになり、例えばソフトウェアのモジュール514と522の間にアプリケーション1、2に跨る参照があっても、これはスロットを跨っていることにより検出が容易となる。

【0056】逆に、アプリケーションごとにスロットとして領域の大きさを事前に規定することは、従来システムに比べ、アプリケーション領域の自由な拡張が難しい、ということが挙げられるが、使用可能な全体領域が限られるICカードにおいては、一般にアプリケーションの基本設計時にほぼその使用領域が決定され、その後自由に拡張されるようなことはない。これは、領域の上限が低いため、動的に領域獲得を行うと容易に領域不足を引き起こしてしまうからである。

【0057】また、物理領域としてスロットを分ける更なる理由の一つとして、一つのアプリケーションが修復不能状態になったとしても、その領域そのものを切り離すことにより、他スロットにあるアプリケーションへの影響は及ばないように実現できる。

【0058】したがって、発行後にアプリケーションのインストールが可能なICカードと、ICカードへの入出力手段となる端末装置を具備するICカードシステムにおいて、各アプリケーションが事前に確定されたスロット内でのみ領域を拡張しうるようにスロット領域を確定することができる。

【0059】また、アプリケーションが使用する領域をそのまま制限された物理領域にマッピングすることにより、領域管理をセキュリティ管理と連動させ、アプリケーションの独立性を領域監視により確保することができる。

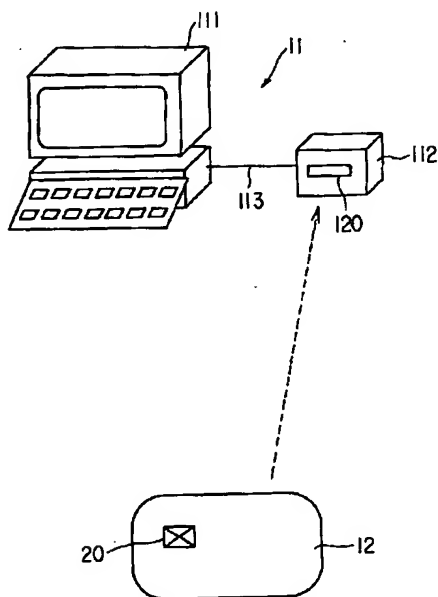
【0060】この構成においては、領域をそのアプリケーションと対応づけることにより、各アプリケーションの独立性を領域単位で保証することを可能とし、高いセキュリティ性をも実現することができる。

【0061】すなわち、ICカードにおいて発行後に載せられる複数アプリケーションを明示的に領域を分割し、管理することにより、他のアプリケーションの好ましくない影響を排除し、アプリケーションごとの柔軟な管理を効率よく実現することができる。

【0062】

【発明の効果】以上詳述したように、この発明によれば、ICカードの発行後に、このICカードに対するアプリケーションのインストールが行えるものにおいて、上記ICカードが不揮発性メモリを有し、上記ICカードにおける各アプリケーションが、事前に確定された上記不揮発性メモリの所定領域としてのスロット内でのみ領域を拡張するようにスロット領域を確定することができるICカード発行システムとICカード処理システムとICカードを提供できる。

【図1】



【図面の簡単な説明】

【図1】この発明の実施形態のICカード発行システムの概略構成を示す図。

【図2】ICカードの概略構成を示すブロック図。

【図3】EEPROMの概略構成を示す図。

【図4】EEPROMのユーザアプリケーション領域の概略構成を示す図。

【図5】スロット管理テーブルの構成例を説明するための図。

【図6】共有テーブルの構成例を説明するための図。

【図7】各スロットとアプリケーションの関係を説明するための図。

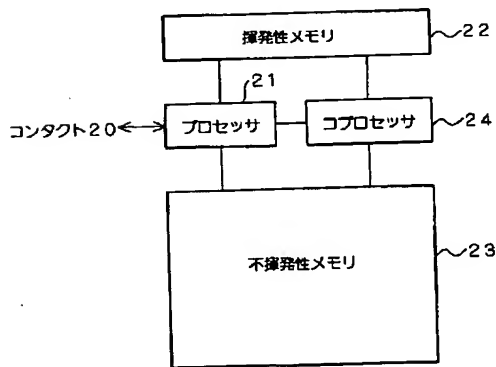
【図8】各アプリケーションのモジュールごとの領域確認処理を説明するためのフローチャート。

【図9】従来の各スロットとアプリケーションの関係を説明するための図。

【符号の説明】

- 11…端末装置
- 12…ICカード
- 21…プロセッサ
- 22…揮発性メモリ(RAM)
- 23…不揮発性メモリ(EEPROM)
- 112…リーダライタ

【図2】

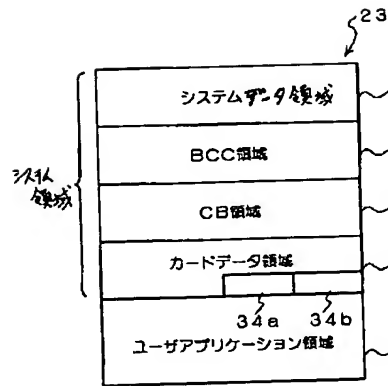


【図6】

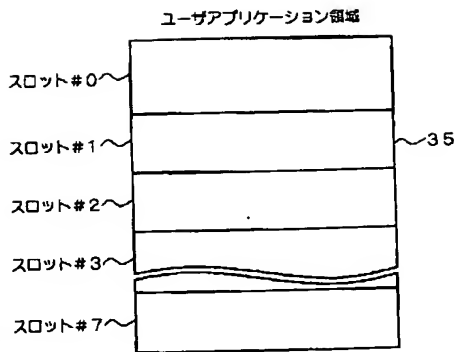
現在処理中のアプリケーション名	現在処理中のモジュール名	許可されるアプリケーション名
AP1	S14	AP2

34b

【図3】



【図4】

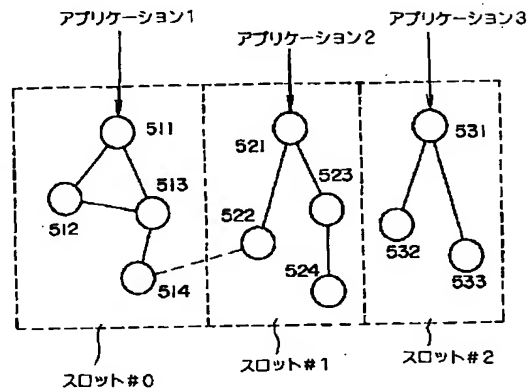


【図5】

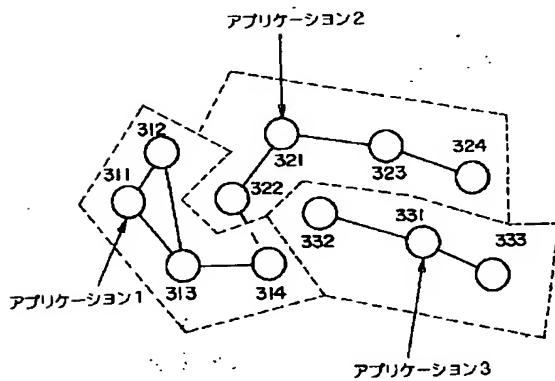
	状態 (STS)	アプリケーション名 (AID)	先頭位置 (TOP)	サイズ (SIZE)
スロット#0				
スロット#1				
スロット#2				
スロット#3				
スロット#4				
スロット#5				
スロット#6				
スロット#7				

34a

【図7】



【図9】



【図8】

